STEGANOGRAFI PADA FRAME VIDEO STATIONER MENGGUNAKAN METODE LEAST SIGNIFICATION BIT (LSB)

Steganography on Stationary Video with Least Significant Bit (LSB) Method

Devi Rahmaditra[1], Dr. Ir. Bambang Hidayat, DEA[2], I Nyoman Apraz Ramatryana, S.T., M.T.[3]
[1,2,3] Prodi Teknik Telekomunikasi Fakultas Teknik Elektro, Telkom University
rahmaditradevi@gmail.com[1] ,avenir.telkom@gmail.com[2], ramatryana@gmail.com[3]

Abstrak

Steganografi merupakan seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Untuk menyembunyikan pesan tersembunyi pada steganografi terdapat beberapa teknik yaitu dengan memilih tempat penyisipan yang aman serta pemilihan metoda penyisipan pesannya. Sehingga dengan pemilihan tempat penyisipan yang tepat serta metoda penyisipan pesan diharapkan akan diperoleh sistem steganografi yang lebih handal.

Dalam tugas akhir ini, dibuat sebuah sistem yang steganografi yang di implementasikan pada sebuah file video digital yang digunakan sebagai *cover*. Dalam penelitian ini steganografi akan ditingkatkan kehanandalannya dengan memlih tempat penyisipan yang lebih tepat. Dimana penelitian kali ini tempat pemilihan tempatnya pada frame yang stasioner.

Dalam penelitian tugas akhir ini telah dibuat sistem steganografi guna mendapatkan keamanan yang tinggi. Teknik penyembunyian diimplementasikan pada media video yang digunakan sebagai cover. Dan didalam video tersebut disisipkan sebuah pesan rahasia berupa teks. Metode yang digunakan adalah *Least Significant Bit* (LSB) karena mudah serta tidak mempengaruhi kualitas media yang digunakan. Video *stego* memiliki performansi yang cukup baik karena PSNR yang didapatkan tinggi, namun ketika diberi serangan performansi sistem kurang baik karena nilai MSE yang didapatkan sangatlah besar.

Kata Kunci: Steganografi, Least Significant Bit, Video

Abstract

Steganography is the art and science of writing hidden messages or hide in a way that besides the sender and the recipient, no one knows or realizes that there is a secret message. To hide the hidden message in steganography, there are several techniques, namely by choosing a safe insertion and the selection method of insertion message. So that with the selection of the proper insertion and method of inserting a message is expected to be obtained steganography system more reliable. Insertion methods that exist among others Insertion Least Significant Bit (LSB), Algorithms and Transformation, Redundant Pattern Encoding, and Spread Spectrum Method. In this study steganography will be enhanced reliability to choose the insertion of a more appropriate place. Where the present study polling stations where the image is stationary.

In this final project has been made steganographic system in order to obtain high security. Concealment techniques implemented in video media being used as a cover. And in the video embedded a secret message in the form of text. The method that used in this system is Least Significant Bit (LSB) as it is easy and does not affect the quality of media used. Video stego has a fairly good performance due to high PSNR obtained, but when the system given attack, the performance is not good because the big rate of MSE.

Keywords: ***Steganography, Least Significant Bit, Video***

1. Pendahuluan

Seiring dengan berkembangnya zaman, memberikan pengaruh yang besar terhadap bagi kehidupan manusia. Perkembangan teknologi jaringan internet memungkinkan setiap orang untuk saling bertukar data, informasi ataupun pesan kepada orang lain tanpa mengenal waktu dan jarak. Dan seiring perkembangan teknologi informasi tersebut, semakin berkembang pula teknik kejahatan yang berupa perusakan maupun pencurian data oleh pihak yang tidak memiliki wewenang atas data tersebut.

Berbagai macam teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak, salah satunya adalah steganografi. Steganografi sebagai suatu seni penyembunyian pesan ke dalam pesan lainnya yang telah ada sejak sebelum masehi dan kini seiring dengan kemajuan teknologi jaringan serta perkembangan dari teknologi digital, steganografi banyak dimanfaatkan untuk mengirim pesan melalui suatu media tanpa diketahui oleh

orang lain. Berbeda dengan kriptografi, steganografi menyimpan suatu pesan dan media lain sebagai pembawa pesan tersebut. Dengan menggunakan steganografi, orang awam tidak menyadari keberadaaan suatu informasi. Metode yang digunakan dalam steganografi ada bermacam macam seperti LSB, REP, SSM.
Dari permasalahan yang ada maka peneliti bermaksud untuk membuat suatu sistem steganografi dengan media video dan metode LSB agar dapat menyisipkan suatu pesan tersembunyi.

2. Landasan Teori

A. Steganografi [3]

Kata steganografi (*steganography) berasal dari bahasa Yunani yaitu steganos yang artinya tersembunyi atau*terselubung dan graphein, yang artinya menulis, sehingga kurang lebih artinya adalah "menulis tulisan yang tersembunyi atau terselubung" (Sellars, 1996).
Teknik steganografi ini sudah ada sejak 4000 tahun yang lalu di kota Menet Khufu, Mesir. Awalnya adalah penggunaan hieroglyphic yakni menulis menggunakan karakter-karakter dalam bentuk gambar. Ahli tulis menggunakan tulisan Mesir kuno ini untuk menceritakan kehidupan majikannya. Tulisan Mesir kuno tersebut menjadi ide untuk membuat pesan rahasia saat ini. Oleh karena itulah, tulisan Mesir kuno yang menggunakan gambar dianggap sebagai steganografi pertama di dunia.(Ariyus, 2009).

B. Least Significant Bit (LSB) [2]

Metoda yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya, pada berkas image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap pixel berkas bitmap 24 bit kita dapat menyisipkan 3 bit data.
Kekurangan dari LSB Invertion: Dapat diambil kesimpulan dari contoh 8 bit pixel, menggunakan LSB Insertion dapat secara drastis mengubah unsur pokok warna dari pixel. Ini dapat menunjukkan perbedaan yang nyata dari cover image menjadi stego image, sehingga tanda tersebut menunjukkan keadaan dari steganografi. Variasi warna kurang jelas dengan 24 bit image, bagaimanapun file tersebut sangatlah besar. Antara 8 bit dan 24 bit image mudah diserang dalam pemrosesan image, seperti cropping (kegagalan) dan compression (pemampatan).
Keuntungan dari LSB Insertion : Keuntungan yang paling besar dari algoritma LSB ini adalah cepat dan mudah. Dan juga algoritma tersebut memiliki software steganografi yang mendukung dengan bekerja di antara unsur pokok warna LSB melalui manipulasi pallete (lukisan).

C. AVI (*Audio Video Intervealed*) [4]

Format file AVI dapat menyimpan data video dan audio dan dapat memainkan kedua jenis data tadi secara bersamaan. AVI memiliki jenis *codec* yang berbeda-beda, seperti halnya MPEG yang memiliki jenis berbeda-beda (MPEG1, MPEG2, MPEG4). Format file AVI termasuk salah satu format yang menggunakan metaformat RIFF yang membagi data ke dalam bagian-bagian atau blok-blok yang disebut "*chunck*".

D. Parameter Pengujian

1. MOS (Mean Opinion Score)

   Mean Opinion Score merupakan rekomendasi ITU P.800 yang digunakan untuk mengukur kinerja dari suatu komunikasi multimedia melalui jaringan berdasarkan pandangan dari responden. responden akan memberikan penilaian dengan range angka 1-5 dimana, angka 1 berarti kualitas yang amat buruk dan angka 5 adalah kualitas yang sangat baik.

Tabel 1. Skala *Mean Opinion Score* [1]

MOS	Quality	Impairment
5	Sempurna	Video terinterpretasi sangat baik
4	Baik	Video terinterpretasi baik, tidak ada kerusakan
3	Cukup	Video masih dapat dikenali, terdapat kerusakan
2	Kurang	Video kurang di mengerti, kerusakan cukup berarti
1	Buruk	Video tidak dapat di interpretasi

2. MSE (*Mean Square Error*) [5]
   MSE adalah nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi. Berikut adalah perhitungannya:

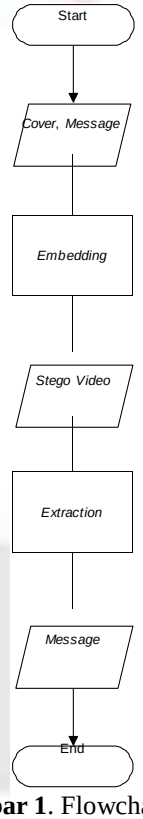
$$MSE = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left| \left(f(x,y) - g(x,y) \right)^2 \right|$$

3. PSNR (*Peak Signal to Noise Ratio*)
   Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan *decibel* (dB).

(——)

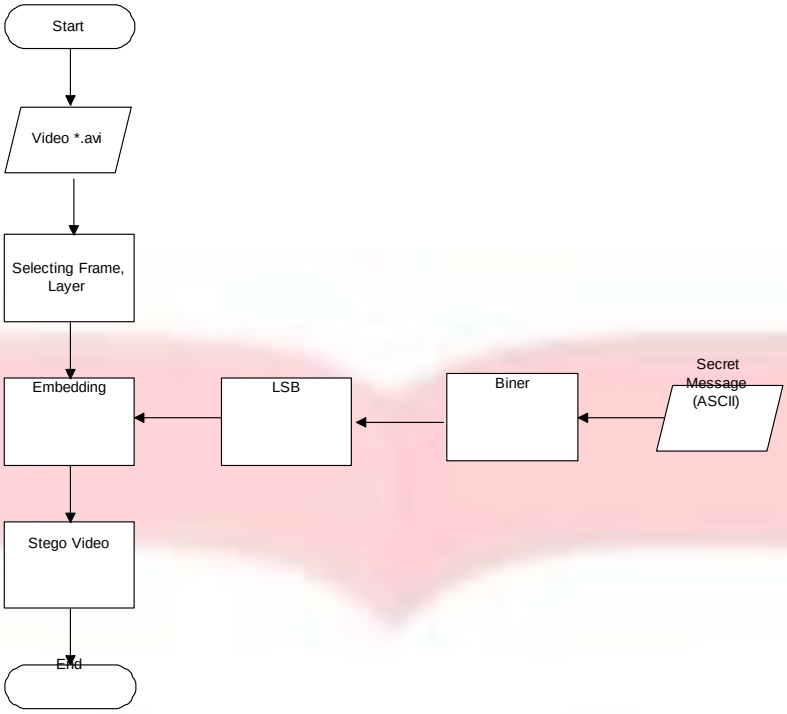
4. BER *(Bit Error Rate)* [6]
merupakan parameter pengujian dimana bagus tidaknya sistem steganografi dan ekstraksi yang telah dibuat didasarkan pada benar atau tidaknya sistem dalam mengekstraksi bit-bit pesan yang telah dikirimkan.

5. Blok Diagram Sistem



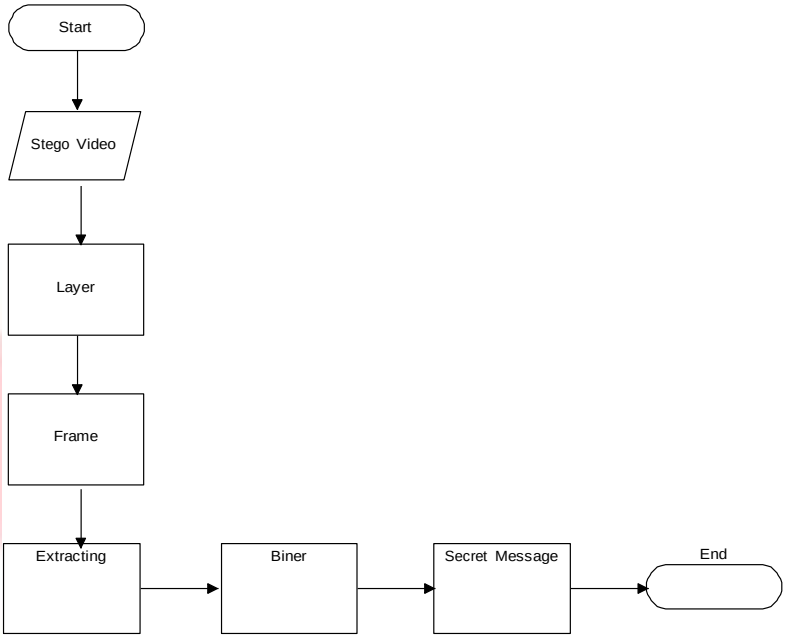
Gambar 1. Flowchart Sistem

Dari gambar diatas menunjukan sistem yang akan dibuat dalam menyisipkan suatu file ke media video. Proses pertama kali yang dilakukan adalah mengupload video yang akan disisipi oleh file *stego*. Video yang akan diupload memiliki durasi maksimal yang sudah ditentukan. Serta memasukkan pesan yang akan disisipkan. Setelah itu dilakukan proses *embedding*, dimana menyisipkan pesan ke dalam video. Hasil dari *embedding* adalah video *stego* yang akan di ekstraksi di proses selanjutnya. Kemudian stego *video* akan di ekstraksi untuk menghasilkan pesan rahasia yang tersimpan di dalam cover *video*.



Proses *embedding* dilakukan di pihak pengirim, sistem ini dapat dijelaskan sebagai berikut:

1. Pengguna memasukan video *cover* yang akan disisipkan pesan rahasia.
2. Pada *selecting frame* dan *layer*, dilakukan proses pemilihan tempat (*frame stationer*) mana yang akan disisipkan serta memilih layer yang akan disisipkan pesan rahasia.
3. Disisi lain, pesan yang telah dimasukkan yang berupa ASCII akan diubah ke dalam bentuk bit-bit (biner). Dan setelah itu dilakukan proses LSB. Pesan yang diubah menjadi bit-bit yang termasuk bit LSB pada tiap *byte* warna untuk setiap *pixel*. Karena layer yang diproses hanya satu layer saja, maka yang diubah bit-bit nya yaitu pada layer *red* saja.
4. Di proses *embedding*, *cover* video yang sudah diproses pemilihan frame dan layer nya akan di embed dengan pesan rahasia yang sudah diubah bit-bit nya dengan metode LSB.
5. Setelah proses penyisipan selesai, selanjutnya *file* video yang berisi pesan rahasia akan ditampilkan, yang selanjutnya disebut video *stego*.

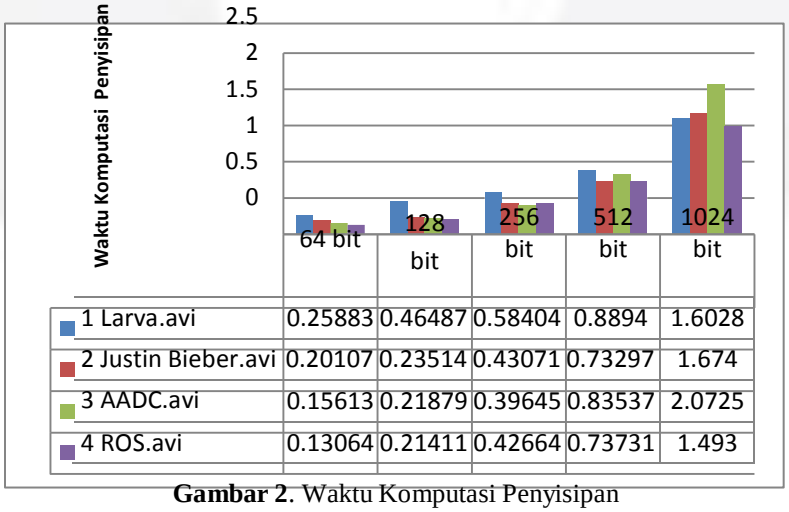


Proses ekstraksi dilakukan oleh pihak penerima, dijelaskan sebagai berikut:

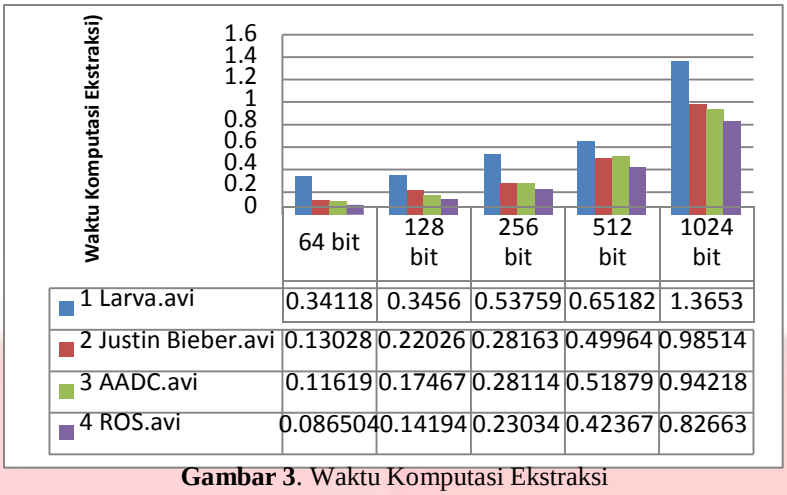
1. Pengguna memasukkan file video yang berisi pesan rahasia. Kemudian sistem akan memeriksa layer mana yang disisipkan pesan, dan frae mana yang dsisipkan pesan.
2. Jika sudah, maka proses ekstraksi terhadap pesan rahasia pada video *stego* akan dilakukan.
3. Pesan rahasia dalam video *stego* akan di ekstraksi menggunakan metode LSB.
4. Proses ekstraksi selesai. Dalam tahap ini, pihak penerima mendapatkan pesan rahasia yang telah dikirim.

3. Pembahasan

1. Pengaruh Panjang Pesan dan Ukuran *Cover* terhadap Waktu Komputasi.
   Panjang pesan dan ukuran *cover* video sangat berpengaruh terhadap waktu komputasi. Pengujian dilakukan pada video *cover* dengan nilai *threshold* 0.2 dan menyisipkan pesan stego yang berukuran 64 bit, 128 bit, 256 bit, 512 bit dan 1024 bit. Berikut grafik waktu komputasi penyisipan dan ekstraksi:



Gambar 2. Waktu Komputasi Penyisipan



Gambar 3. Waktu Komputasi Ekstraksi

Dari pengujian yang telah dilakukan, semakin besar ukuran pesan yang di sisipkan pada *cover*, maka semakin besar waktu komputasi yang dibutuhkan. Hal ini terjadi karena semakin besar ukuran pesan yang disisipkan, maka semakin banyak pesan yang harus disisipkan sehingga membutuhkan waktu yang lama dalam proses steganografi. Selain itu, ukuran *cover* juga mempengaruhi waktu komputasi yang dibutuhkan dalam penyisipan dan ekstraksi. Semakin besar ukuran *cover* yang digunakan, maka semakin lama pula waktu komputasi yang dibutuhkan.

2. Ketahanan Sistem Terhadap Serangan *Noise*

Performansi ketahanan sistem dapat dilakukan pengujian dengan memberikan serangan *noise* pada *stego* oise yang digunakan adalah *Gaussian* dan *Salt and Pepper noise*. Video yang digunakan adalah AADC.avi dengan ukuran *frame* 150x180 yang akan disisipkan dengan pesan sepanjang 64 bit. Berikut adalah hasil pengujian sistem yang telah diberikan serangan *Salt and Pepper* dan *Gaussian noise*:

Tabel. 2 Pengujian dengan *Salt and Pepper Noise*

No	Parameter	tanpa *noise*	0.0001	0.001	0.01	0.1
1	MSE	0.887243	3.17849	23.7547	231.176	2301.19
2	PSNR	48.6504	43.1086	34.3733	24.4914	14.5113

Berdasarkan hasil pengujian pada AADC.avi nilai MSE yang didapatkan sebelum diberi serangan *Salt and Pepper* adalah 0.887243 sedangkan untuk PSNR adalah 48.6504 dB. Berdasarkan tabel diatas semakin besar serangan *Salt and Pepper* yang diberikan kepada video, maka semakin besar nilai MSEnya. Hal ini berbanding terbalik dengan nilai PSNR, yakni semakin besar nilai serangan *Salt and Pepper* yang diberikan maka semakin kecil nilai PSNR yang didapatkan.

Tabel.3 Pengujian dengan *Gaussian Noise*

No	Nama	tanpa *noise*	0.0001	0.001	0.01	0.1
1	MSE	0.887243	548.06	548.792	561.512	1159.89
2	PSNR	48.6504	20.7425	20.7367	20.6372	17.4866

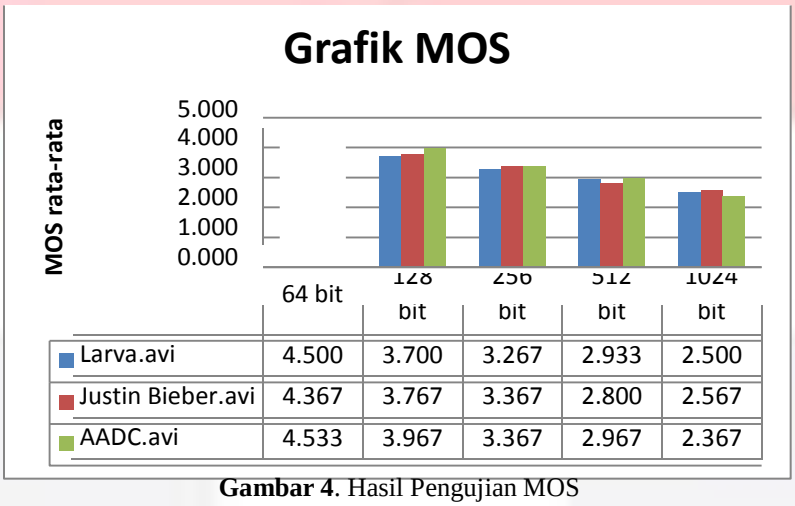
Berdasarkan hasil pengujian pada AADC.avi nilai MSE yang didapatkan sebelum diberi serangan *Gaussian* adalah 0.887243 sedangkan untuk PSNR adalah 48.6504 dB. berdasarkan tabel diatas semakin

besar serangan *Gaussian* yang diberikan kepada video, maka semakin besar nilai MSEnya. Hal ini berbanding terbalik dengan nilai PSNR, yakni semakin besar nilai serangan *Gaussian* yang diberikan maka semakin kecil nilai PSNR yang didapatkan.

Besar *noise* yang diberikan sangat mempengaruhi nilai MSE dan PSNR. Semakin besar *noise* (*Salt and Pepper* atau *Gaussian*) yang diberikan maka semakin besar nilai MSE yang didapatkan, namun nilai PSNR yang didapatkan berbanding terbalik. BER yang didapatkan dari kedua jenis pengujian ini adalah 68.0703.

3. Pengujian Terhadap MOS

Nilai MOS yang diperolah tidak harus bilangan bulat. Teknisnya 30 orang diminta untuk menonton video pkan pesan yang berbeda-beda. Setiap orang diminta untuk menilai kualitas video tersebut dari rentang 1 sampai dengan 5. Nilai 1 menyatakan nilai yang paling buruk dan 5 untuk yang menyatakan yang paling baik. Berikut ini adalah tabel hasil uji coba yang dilakukan terhadap tiga video berformat *.avi:



Gambar 4. Hasil Pengujian MOS

Dari hasil pengujian diatas, dapat dilihat bahwa kelima pengujian dengan tiga video yang berbeda mendapatkan nilai MOS dengan kualitas yang baik pada penyisipan teks 64 bit, sedangkan cukup pada penyisipan 128 bit, dan 256 bit, sedangkan pada penyisipan 512 bit dan 1024 bit *video stego* mendapatkan nilai MOS yang kurang baik. Melalui pengujian secara subjektif dapat disimpulkan bahwa penyisipan pesan ke dalam video memiliki kualitas berbeda, tergantung dari jumlah bit yang disisipkan.

4. Kesimpulan

Dari hasil analisis pengujian sistem steganografi pada frame video stasioner di dapatkan hasil bahwa:

1. Semakin besar ukuran pesan yang di sisipkan pada *cover*, maka semakin besar waktu komputasi yang dibutuhkan. Selain itu, ukuran *cover* juga mempengaruhi waktu komputasi yang dibutuhkan dalam penyisipan dan ekstraksi. Semakin besar ukuran *cover* yang digunakan, maka semakin lama pula waktu komputasi yang dibutuhkan. Hal ini dapat dilihat pada penyisipan dengan 1024 bit ke video *cover* membutuhkan waktu 2.0725 sekon (pada AADC.avi) dan untuk ekstraksi membutuhkan waktu komputasi 1.3653 sekon (pada Larva.avi).
2. Semakin besar serangan *Salt and Pepper* yang diberikan kepada video, maka semakin besar nilai MSEnya, hal ini berbanding terbalik dengan nilai PSNR, yakni semakin besar nilai serangan *Salt and Pepper* yang diberikan maka semakin kecil nilai PSNR yang didapatkan.
3. Semakin besar serangan *Gaussian* yang diberikan kepada video, maka semakin besar nilai MSEnya. Hal ini berbanding terbalik dengan nilai PSNR, yakni semakin besar nilai serangan *Gaussian* yang diberikan maka semakin kecil nilai PSNR yang didapatkan.
4. Kelima pengujian dengan tiga video yang berbeda mendapatkan nilai MOS dengan kualitas yang baik pada penyisipan teks 64 bit, sedangkan cukup pada penyisipan 128 bit, dan 256 bit, sedangkan pada penyisipan 512 bit dan 1024 bit *video stego* mendapatkan nilai MOS yang kurang baik.

Daftar Pustaka:

[1] Abdi, Nailul Mustaqim, dkk. 2011. "*Peningkatan Kualitas Citra Digital Menggunakan Metode Super Resolusi Pada Domain Spasial*". Jurusan Teknik Elektro, Unsyiah, Banda Aceh.

[2] Alatas, Putri. 2009. "*Implementasi Teknik Steganografi dengan Metode LSB Pada Citra Digital".* Jurusan Sistem Informasi, Universitas Gunadarma, Jakarta.

[3] Berg G, Davidson, Ming-Yuan Dual, Paul G. 2003. "*Searching For Hidden Message: Automatic Detection of Steganography*". Washington: Computer Science Departement, University at Albany.

[4] Rekamasanti, Farisah Qisthina. 2015. "*Implementasi dan Analisis Video Steganografi dengan Format Video AVI Berbasis LSB (Least Significant Bit) dan SSB-4 (System of Steganography Using Bit 4)".* Bandung

[5] Syarifuddin, Sony Nuryadin. 2006. "*Analisis Filtering Citra dengan Metode Mean Filter dan Median Filter*. Jurusan Teknik Informatika, Universitas Komputer Indonesia, Bandung.

[6] Wahid, Muhammad Luthfi. 2015. "*Analisis dan Simulasi Steganografi Video Berbasis Deteksi Band Frekuensi Menggunakan Metode Discrete Wavelet Transform*". Fakultas Teknik Elektro, Universitas Telkom.